防衛装備庁

ソフトウェア耐タンパー技術の研究

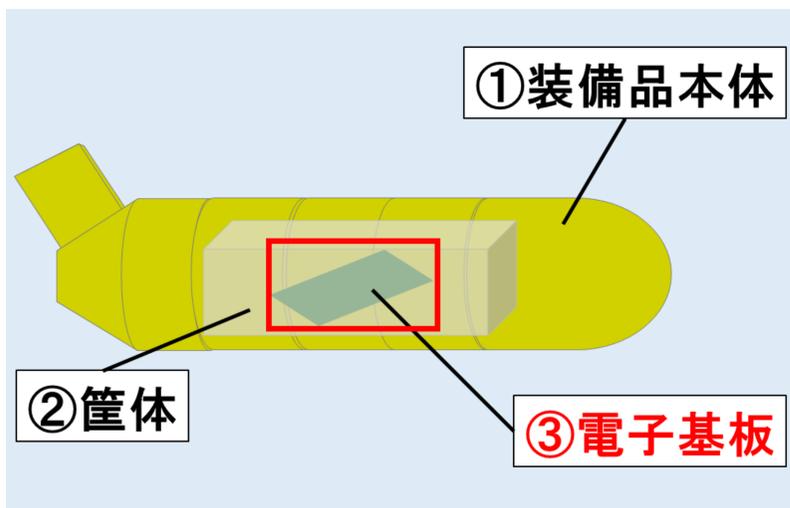
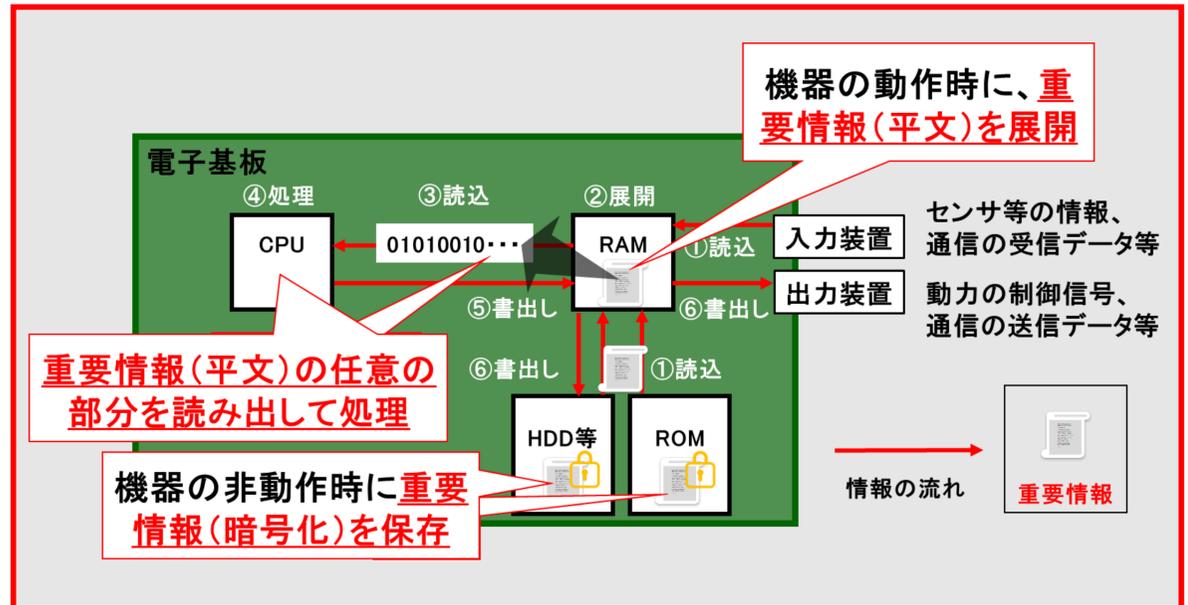
防衛装備庁　新世代装備研究所　AI・サイバーネットワーク研究部　サイバーセキュリティ研究室

研究背景及び研究目的

- ■ 無人機の鹵獲や輸出等によって、第三者からソフトウェアを不正に解析された場合、防衛省・自衛隊の暗号アルゴリズム等の重要情報が漏洩する可能性がある。
- ■ ソフトウェア解析対策としてソフトウェア耐タンパー技術※1があるが、有効な対策方法を統一的に定めた基準等は存在しない。
- ■ ソフトウェア耐タンパー技術の有効性を評価・整理し、ソフトウェア耐タンパー技術の実装要領をまとめたソフトウェア解析対策の指針を作成する。
- ■ 本研究はR3～R5にかけて実施。

※1　ソフトウェアの機能（プログラムを複雑化等）により、不正な解析を防止する技術。

ソフトウェア耐タンパー技術の必要性

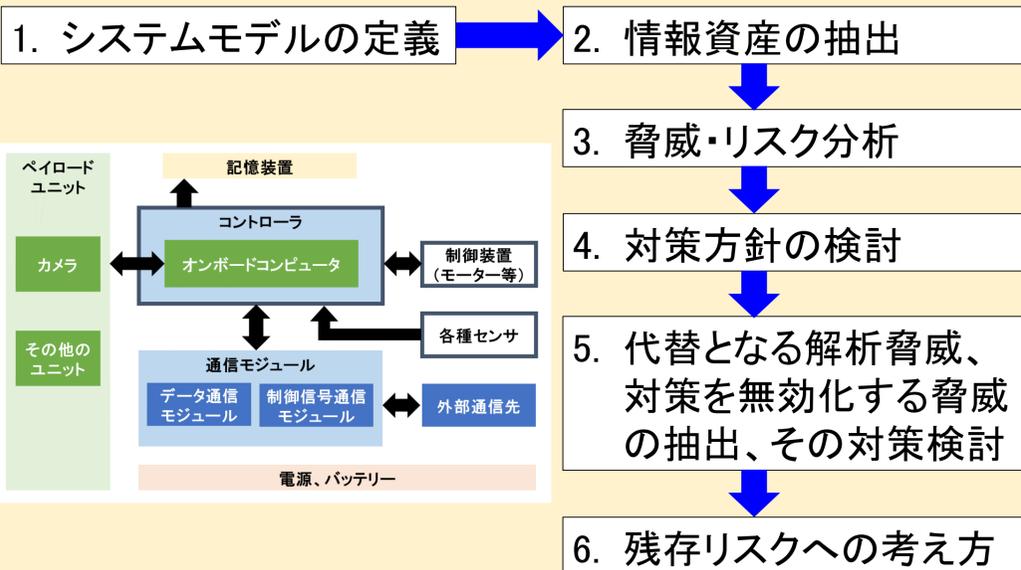
- ■ 装備品の重要情報が保存・処理されるのが、③電子基板である。
- ■ 電子基板上で情報が処理される際、重要情報は平文に展開されるため解析が容易。
- ■ 機器の動作時も含めて保護できるソフトウェア耐タンパー技術の実装が必要。

装備品の構成の概略

電子基板の構成と重要情報を処理する流れの概略

研究成果

- ■ ソフトウェア解析対策の指針に基づいて対策することで、十分な解析対策効果が得られることを確認。
- ■ ソフトウェア耐タンパー技術を決定するための考え方をまとめたソフトウェア解析対策の指針を作成。
  ⇒部内への公開を検討中

ソフトウェア解析対策の指針

1. システムモデルの定義
2. 情報資産の抽出
3. 脅威・リスク分析
4. 対策方針の検討
5. 代替となる解析脅威、対策を無効化する脅威の抽出、その対策検討
6. 残存リスクへの考え方

ペイロードユニット
記憶装置
コントローラ
オンボードコンピュータ
カメラ
制御装置（モーター等）
その他のユニット
各種センサ
通信モジュール
データ通信モジュール
制御信号通信モジュール
外部通信先
電源、バッテリー

以下の知識・経験を有する解析者2名による解析結果

- マルウェア調査・解析
- 脆弱性調査・検査

解析者	対象ソフトウェア	解析可否	解析実績時間
A	ソフトウェア①	×	24時間
B	ソフトウェア②	×	21時間
B	ソフトウェア③	×	28時間

⇒少なくとも数ヵ月での解析は困難との考察※2も得られた。

※2　解析者らの経験値を踏まえた考察。